LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Zero-Day Attacks

11/18/2021

TLP: WHITE, ID# ***202111181300***

Agenda

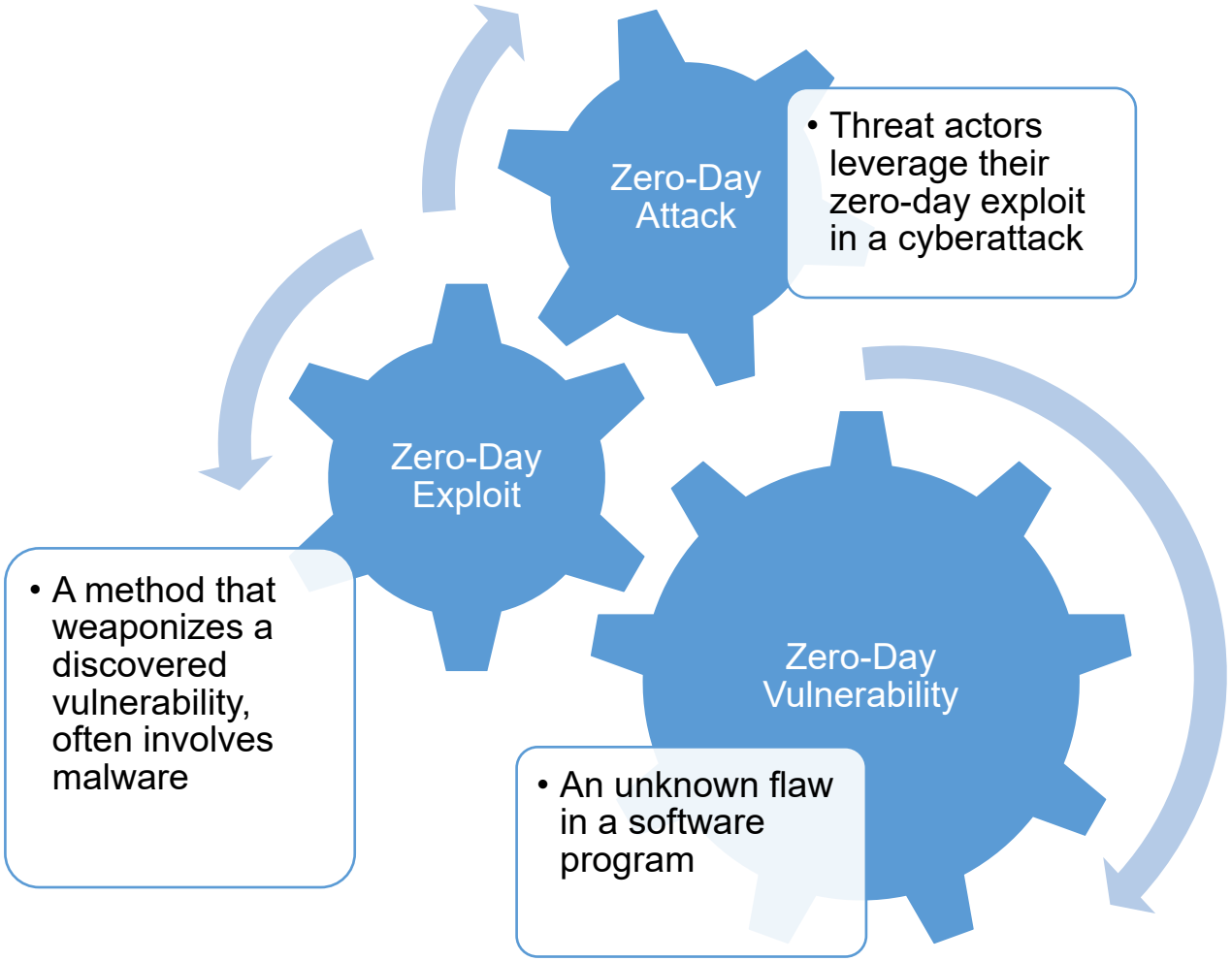
- What are Zero-Day Attacks?
- Famous Attacks Leveraging Zero-Days
- Zero-Day Trends
- Bug Bounty Programs
- Impact on the HPH sector
- Mitigations

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

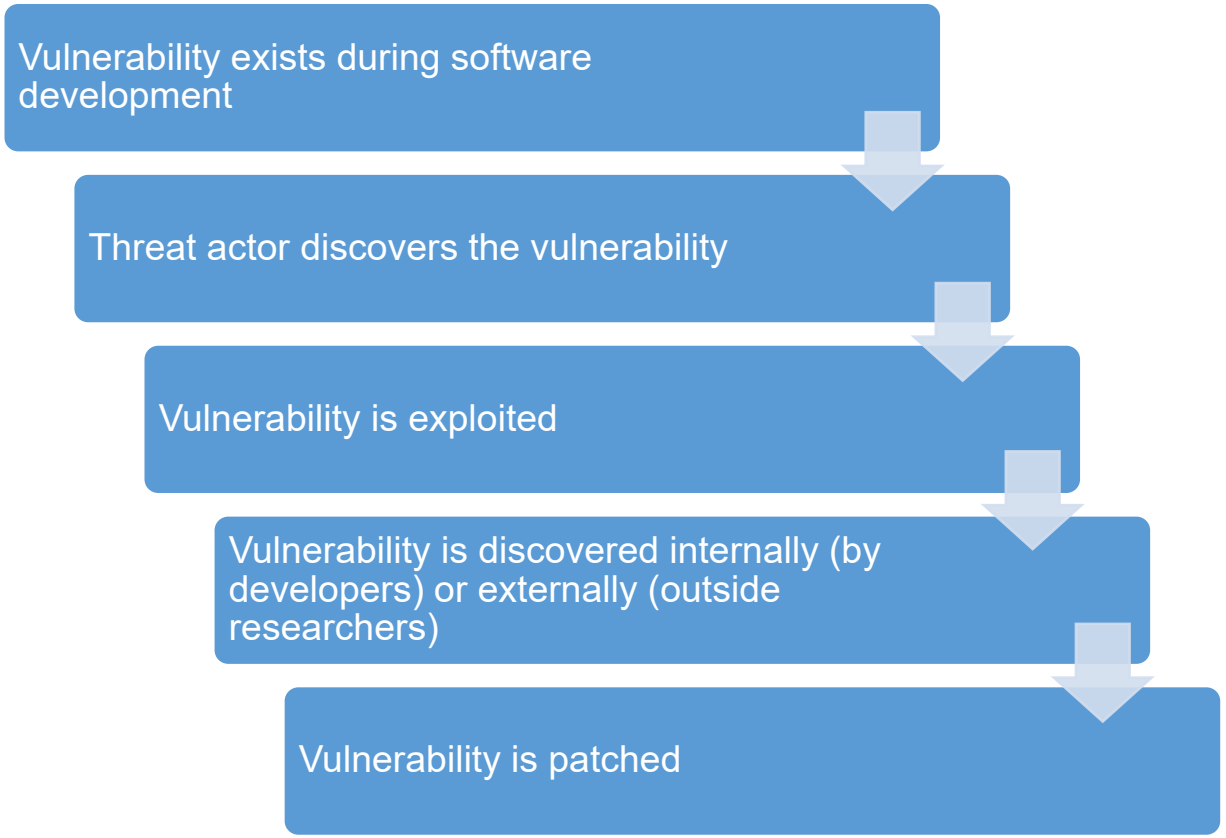
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What We Mean When We Say "Zero-Day"



Zero-Days

- Collectively, a zero-day attack is a vulnerability that is exploited by threat actors before a patch is developed and applied.
- Because no time exists between when the vulnerability is discovered by developers and when it is exploited by threat actors, these vulnerabilities are called “zero-days”.



- 2010 Stuxnet attack on Iranian nuclear program
  - Four zero-days
  - Successfully caused Iranian centrifuges to self-destruct, damaging Iran's nuclear program
- 2017 Dridex Trojan
  - Emails in this campaign used an attached Microsoft Word RTF (Rich Text Format) document and led to installation of the Dridex botnet on devices
  - Avoided common malware-blocking mitigations and did not require user interaction beyond opening the document
  - Patched on April 11, 2017
- 2021 SonicWall zero-day ransomware attack
  - UNC2447 used vulnerability in SonicWall SMA 100 Series VPN to deploy FiveHands ransomware
    - FiveHands, HelloKitty, and DeathRansom ransomwares are in the same family
  - Later exploited indiscriminately in the wild
  - SonicWall released mitigations in February 2021

HAFNIUM

- January 2021 HAFNIUM attack on Microsoft Exchange servers
  - Collection of four zero-days
    - Threat actors look for internet-accessible Microsoft Exchange servers using Outlook Web Access (OWA), then create a web shell to gain remote control of the compromised server
    - Once compromised, threat actors can steal an organization's data, gain unauthorized access to critical systems, elevate privileges, and move laterally to other systems and environments
  - Originally accomplished by Chinese state-sponsored group
    - Expanded to at least ten APT groups by mid-March, including six groups exploiting the vulnerability before a patch was created
    - Possible convergent discovery, more likely purposeful distribution
  - Affected over 100,000 mail servers
    - Targeted organizations included biotechnology, pharmaceutical, and healthcare entities
  - Patched in March 2021
    - Patch prevents new organizations from being compromised, does not solve existing infiltration

Surveyed approximately 400 IT and IT security practitioners located in the United States in 2019

100%

- The amount that new or unknown zero-day attacks were expected to increase from 2019 to 2020

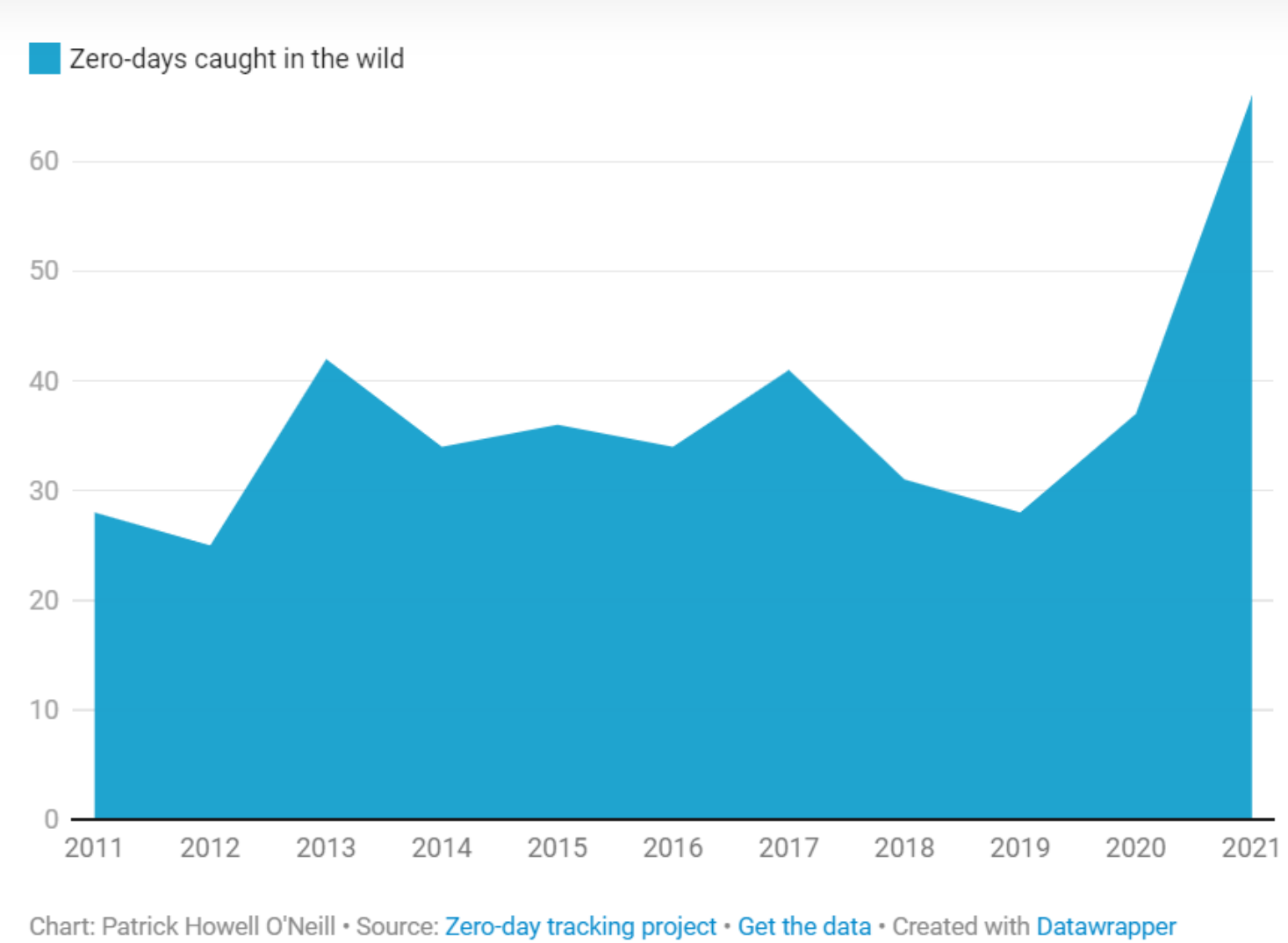
80%

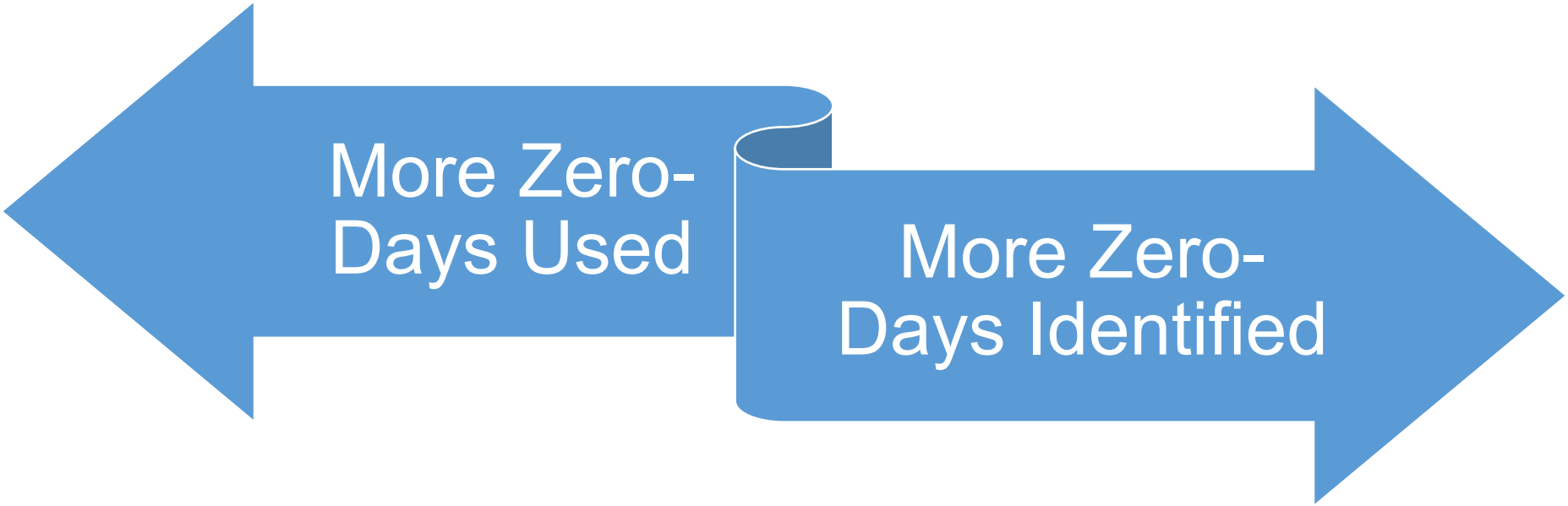
- The percentage of successful breaches that are new or unknown zero-days
- These attacks either involved the exploitation of undisclosed vulnerabilities, or the use of new malware variants that detection solutions do not recognize

97 Days

- The average time to apply, test and fully deploy patches

MIT Research Identifies Zero-Day Trends




More Zero-Days Used
More Zero-Days Identified

More Zero-Days Used vs. Identified

More Used:

- Zero-day exploits are incredibly valuable
  - >$1 million on open market
  - Zerodium's public zero-day prices shows as much as a 1,150% rise in the cost of the highest-end hacks from 2018-2021
- Market for zero-days is opening up
  - Previously limited to groups with deep pockets
  - "If you can't develop your own zero-days, store-bought is fine"
- **"Financially motivated actors are more sophisticated than ever. One-third of the zero-days we've tracked recently can be traced directly back to financially motivated actors."** – Jared Semrau, Director of Vulnerability and Exploitation at FireEye Mandiant
  - Zero-days can be leveraged into lucrative attacks, such as ransomware
- A single vulnerability can put millions of customers at risk

More Identified:

- Consensus of security researchers is that increased rate of detection is driving at least part of this trend
- **"Defenders have clearly gone from being able to catch only relatively simple attacks to detecting more complex hacks."** – Mark Dowd, founder of Azimuth Security.
- Increase in quality and availability of detection tools
- Private sector groups devote massive resources to the problem
  - Google's Threat Analysis Group (TAG)
  - Kaspersky's Global Research & Analysis Team (GReAT)
  - Microsoft's Threat Intelligence Center (MSTIC)
- Bug bounty programs provide financial rewards for turning in vulnerabilities rather than exploiting them

Bug Bounty Programs

- Vendors may reward hackers directly for flaws with their products
  - In October 2021, blockchain technology company Polygon paid 2 million USD to an ethical hacker for his discovery of a flaw that would have allowed a hacker to make repeated double-withdrawals from their network
- Third parties may act as intermediaries between hackers and software companies
  - Examples: Zerodium and Zero Day Initiative
  - Can preserve security researcher anonymity and privacy
  - Acquiring company owns the rights to the zero-day exploit and any intellectual property
  - Resells information to affected vendors

- August 2021 discovery of zero-day vulnerability “PwnedPiper” affecting the pneumatic tube systems used by hospitals to transport medication, bloodwork, and test samples
  - Attackers could exploit flaws in the control panel software
    - Control panel allowed unsigned, as well as unauthenticated and unencrypted, firmware updates
    - Hard coded credentials could allow attackers access
    - Required physical access to the panel
  - "The Nexus Control Panel powers the stations on-premises. Once you compromise a station, without [needing] credentials, you can harvest any employee credentials to access these systems.” – Ben Seri, Vice President of Research at Armis
  - Network segmentation can mitigate this vulnerability

- Zero-day attacks can be used both to target specific, high value targets or affect wide swathes of organizations through commonly used software
  - Both pose substantial dangers to the HPH sector
- The most effective mitigation for zero-day attacks is patching, which can be difficult on medical IOT or legacy systems
- August 2020: Zero-day vulnerabilities in healthcare records application OpenClinic exposed patients' test results
  - Developers were unresponsive to reports of four zero-days
  - Due to lack of developer action, users were urged to stop using the open-source program
  - Unauthenticated attackers could successfully request files containing sensitive documents from the medical test directory, including medical test results
    - Files must be requested by name

Mitigations

- Mitigating zero-day attacks completely is not possible – by nature, they are novel and unexpected attack vectors
- **Patch early, patch often, patch completely**
  - Security resources like HC3 can provide insight into active zero-days and available patches
- Implementing a web-application firewall to review incoming traffic and filter out malicious input can prevent threat actors from reaching security vulnerabilities
  - Analyzes traffic to and from applications, but not activity within applications
  - Requires considerable effort to monitor and "tune" to correctly identify malicious and non-malicious inputs
- Runtime application self-protection (RASP) agents sits inside applications' runtime
  - RASP's ability to detect anomalous behavior can prevent threat actors from executing zero-days

Reference Materials

References

- "What is a Zero-Day Exploit?" FireEye. October 28, 2021. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
- "Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day," Proofpoint. April 11, 2017. https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day
- Gatlin, Sergiu. "New ransomware group uses SonicWall zero-day to breach networks," Bleeping Computer. April 29, 2021. https://www.bleepingcomputer.com/news/security/new-ransomware-group-uses-sonicwall-zero-day-to-breach-networks/
- Abrams, Lawrence. "SonicWall SMA 100 zero-day exploit actively used in the wild," Bleeping Computer. February 1, 2021. https://www.bleepingcomputer.com/news/security/sonicwall-sma-100-zero-day-exploit-actively-used-in-the-wild/
- Deuby, Sean. "Timeline of a Hafnium Attack," Security Boulevard. May 5, 2021. https://securityboulevard.com/2021/05/timeline-of-a-hafnium-attack/
- Flesher, Michael. "Healthcare's Microsoft Exchange Critical Exposure," Meditology Services. March 15, 2021. https://www.meditologyservices.com/healthcares-microsoft-exchange-critical-exposure/
- Ponemon, Larry. "The state of endpoint security risk: it's skyrocketing," Ponemon Institute. May 2020. https://ponemonsullivanreport.com/2020/05/
- Ponemon Institute. "The Third Annual Study on the State of Endpoint Security Risk," Morphisec. January 2020. https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

References

- O'Neill, Patrick. “2021 has broken the record for zero-day hacking attacks,” MIT Technology Review. September 23, 2021. https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/
- O'Neill, Patrick. “This US company sold iPhone hacking tools to UAE spies,” MIT Technology Review. September 15, 2021. https://www.technologyreview.com/2021/09/15/1035813/us-sold-iphone-exploit-uae/
- Haworth, Jessica. “Bug Bounty Radar // The latest bug bounty programs for November 2021,” Port Swigger. November 1, 2021. https://portswigger.net/daily-swig/bug-bounty-radar-the-latest-bug-bounty-programs-for-november-2021
- “What Is Runtime Application Self-Protection (RASP)?” CheckPoint Security. November 1, 2021. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-runtime-application-self-protection-rasp/
- “Zero-day (0day) exploit,” Imperva. November 1, 2021. https://www.imperva.com/learn/application-security/zero-day-exploit/
- Goodin, Dan. “There’s a vexing mystery surrounding the 0-day attacks on Exchange servers,” Ars Technica. March 11, 2021. https://arstechnica.com/gadgets/2021/03/security-unicorn-exchange-server-0-days-were-exploited-by-6-apts/
- Bannister, Adam. “Zero-day vulnerabilities in healthcare records application OpenClinic could expose patients’ test results,” PortSwigger. December 2, 2020.
- Jackson Higgens, Kelly. “Multiple Zero-Day Flaws Discovered in Popular Hospital Pneumatic Tube System,” Dark Reading. August 2, 2021. https://www.darkreading.com/vulnerabilities---threats/multiple-zero-day-flaws-discovered-in-popular-hospital-pneumatic-tube-system/d/d-id/1341584

Questions

Upcoming Briefs

- 12/2 – FIN12 as a Threat to Healthcare

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV